Davis Wright Tremaine LLP

1919 Pennsylvania Avenue N.W.
Suite 800
Washington, D.C. 20006-3401

Christopher Ott
1.202.973.4221 tel
ChrisOtt@dwt.com

October 2, 2019

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Re: Security Breach Notification

Dear Office of the Attorney General:

I am writing you on behalf of Ampersand, located at 151 West 42nd Street, 11th Floor, New York, NY 10036, pursuant to Md. Code Ann. Comm. Law 14-3504.

On August 7, 2019, Ampersand discovered that an employee accessed certain employee records containing sensitive information without authorization. Forensic analysis revealed that the unauthorized access had been occurring since July 10, 2019. The employee claimed to be accessing salary information to leverage the information to receive an increase in compensation.

Upon discovering this access, Ampersand conducted a forensic examination of both the shared drive and the employee's computer. The Company determined that the employee accessed a number of files with sensitive information without authorization and then attempted to mislead the Company regarding this access. After extensive analysis and meeting with Human Resources, the employee was fired. Ampersand has modified its access controls to limit access to the sensitive information.

On September 11, 2019, Ampersand confirmed that the personal information of eleven (11) Maryland residents may have been impacted by the data incident. Ampersand has found no evidence that the personal information was misused. Ampersand will send written notice by U.S. mail to impacted individuals on October 3, 2019. A copy of this notice is enclosed. As referenced in the letter, consumers will be provided with **12 months** of credit monitoring to affected consumers through **Kroll**.

We assure you that our client, Ampersand, takes this issue, and the privacy and security of its customers, very seriously and is working diligently to ensure that this does not occur again. Please feel free to contact me if you have any questions: **(202) 973-4221** or at **ChrisOtt@dwt.com**.

Warm regards,

Chris Ott

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

NOTICE OF DATA BREACH

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to tell you about a data security incident that resulted in the unauthorized access to and/or acquisition of your personal information. In an abundance of caution, we are providing you with credit monitoring services, as described below. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

WHAT HAPPENED?

On August 7, 2019, Ampersand discovered that an employee accessed certain employee records containing sensitive information, including yours, without authorization. Upon discovering this access, we conducted a forensic examination of both the drive the information was stored on and the employee's computer. We have determined that the employee accessed a number of files with sensitive information without authorization. Forensic analysis revealed that the unauthorized access had been occurring since July 10, 2019.

WHAT INFORMATION WAS INVOLVED?

Information in the accessed files included name, Social Security number, and salary information.

WHAT WE ARE DOING:

We investigated the incident to determine the breadth of access and if anyone else accessed information outside of the scope of their responsibilities; we determined that the unauthorized access was limited to a single employee. We have reviewed the access controls to the accessed sensitive information and adjusted those controls accordingly.

We have referred this matter to law enforcement. Should you need the police report number, it will remain on file with Human Resources.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Online Single Bureau Credit Monitoring will be provided to all notified individuals for 12 months. The credit data comes from one of the national credit bureaus. This service can be accessed immediately online. Credit activity will be reported promptly to an Activated Member via email. Monitoring does not affect an individual's credit score, nor does it appear as a hard inquiry on his or her credit report when the credit report is accessed by a third party.

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.
*You have until **January 5, 2020** to activate your identity monitoring services.*
Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

WHAT YOU CAN DO:

We want to ensure that you have the necessary information to take preventive steps to help protect yourself from identity theft.

Please note: Following activation, additional steps are required by you in order to activate your fraud alerts, and to pull your credit score and credit file.

Please review the enclosed "Steps You Can Take to Further Protect Your Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

As always, we encourage you to regularly review and monitor your financial statements and credit reports, and report any suspicious or unrecognized activity immediately. You should be vigilant for incidents of fraud and identity theft and report any suspected incidents of fraud to the relevant financial institution, local law enforcement, your state Attorney General, or the Federal Trade Commission.

FOR MORE INFORMATION:

Further information about how to guard against identity theft appears on the next page. Should you have any questions, please contact 1-866-775-4209, Monday through Friday, from 8 a.m. to 5:30 p.m. Central Time.

We deeply regret any inconvenience this may cause you.

Sincerely,

Deb Josephs
Chief People Officer

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Obtain a Copy of Your Credit Report. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Place a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for up to a year. Identity theft victims can also get an extended fraud alert for up to seven years. Military members have additional benefits and should contact the credit reporting agencies for further questions. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Place a Security Freeze on Your Credit File. As of September 21, 2018, a new federal law allows consumers to freeze and unfreeze their credit file free of charge at all three major credit bureaus. A freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each consumer reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorney General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Penn. Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			